UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

TERESA BUSHEK, individually and on behalf of all others similarly situated, Plaintiff, v. ABC LEGAL SERVICES, LLC, Defendant.	**Case No. 2:24-cv-02117** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Teresa Bushek ("Plaintiff"), individually and on behalf of all other similarly situated individuals, and by and through her undersigned counsel files this Class Action Complaint against Defendant ABC Legal Services, LLC ("ABC" or "Defendant") and alleges the following based upon her personal knowledge of the facts, upon information and belief, and based upon the investigation of her counsel.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against ABC for its negligent failure to protect and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information ("PII") culminating in a massive and preventable data breach (the "Data Breach" or "Breach"). As a result of ABC's insufficient data security, cybercriminals easily infiltrated ABC's inadequately protected computer systems and stole the PII of Plaintiff and the Class (approximately **39,965** individuals).[1]

2. On or around August 7, 2024, ABC detected unusual activity on its network environment.[2] After learning of the issue ABC initiated an investigation.[3] The investigation revealed that certain files were likely taken from its network, including the PII of Plaintiff and the Class.[4]

3. Plaintiff and the Class Members (as further defined below) have had their personally identifiable information stolen as a result of ABC's inadequately secured computer network. ABC betrayed its obligations to Plaintiff and the other Class Members by failing to properly safeguard and protect their PII, thereby enabling cybercriminals to steal their valuable and sensitive information.

4. For the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their PII. Plaintiff and Class Members will have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things,

---

[1] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b7f2187e-3ceb-4f2e-b48e-f697fdd84918.html.

[2] *See* Ex. 1 (Plaintiff's Notice of Data Breach Letter).

[3] *Id.*

[4] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their PII, and/or additional damages as described below.

5. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

I. THE PARTIES

6. Plaintiff **Teresa Bushek** is domiciled in and a citizen of the state of Texas. Plaintiff received a Notice of Data Breach letter ("Notice Letter") from ABC dated December 6, 2024, informing her that her email address and Social Security were accessed and/or acquired by an unauthorized person.[5]

7. Defendant **ABC Legal Services, LLC** is a company incorporated in Washington, with its principal place of business located at 1099 Stewart Street, Suite 700, Seattle, Washington, 98101-2161.

II. JURISDICTION AND VENUE

8. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

9. This Court has personal jurisdiction over Defendant because it is headquartered in and/or operates within this District and regularly transacts business, has agents, and is otherwise within this District.

[5] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

10. Venue is likewise proper as to Defendant in this District because a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

III. FACTUAL ALLEGATIONS

A. ABC's Massive and Preventable Data Breach.

11. ABC provides legal solutions in the United States, including service of process, e-filing, skip tracing, appearance counsel, and venue selection.[6] In that capacity, ABC Legal receives certain files that contain personal information relating to individuals from its customers.[7]

12. By collecting the PII of Plaintiffs and the Class ABC undertook a duty to safeguard and protect Plaintiff's and the Class's PII.

13. On August 7, 2024, ABC detected unusual activity in its network environment.[8]

14. After an investigation, ABC determined that an unknown actor gained access to certain parts of its network for an undisclosed period of time.[9] The investigation also revealed that certain files were likely taken from its network by an unauthorized actor on August 7, 2024.[10]

15. ABC determined that the following types of PII were impacted by the Data Breach: name of individual; Social Security number information; driver's license number; government-issued id number (e.g. passport, state id card); financial information (e.g. account number, credit or debit card number); health insurance information; and date of birth.[11]

16. In other words, cybercriminals obtained everything they could possibly want to commit identity theft and fraud.

---

[6] *See* https://www.abclegal.com/about.

[7] Ex. 1.

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

17. Despite learning of the Data Breach in August 2024, ABC waited to notify victims of the Data Breach until December 2024.[12]

18. All in all, ABC failed to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' PII from unauthorized disclosure. ABC's actions represent a flagrant disregard of the rights of the Class Members, both as to privacy and property.

B. Plaintiff's Experience.

Plaintiff Teresa Bushek

19. Plaintiff Bushek received a Notice of Data Breach Letter from ABC dated December 6, 2024, informing her that her email address and Social Security number were accessed and/or acquired by an unauthorized person.[13]

20. By soliciting and accepting Plaintiff Bushek's PII, ABC agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

21. ABC was in possession of Plaintiff Bushek's PII before, during, and after the Data Breach.

22. Following the Data Breach, Plaintiff Bushek made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity, and reviewing her credit reports. In total, Plaintiff Bushek estimates she has already spent hours responding to the Data Breach. Plaintiff Bushek will be forced to expend additional time to review her credit reports and monitor her accounts for the rest of her life. This is time, spent at Defendant's direction, which has been lost forever and cannot be recaptured.

23. Plaintiff Bushek places significant value in the security of her PII and does not readily disclose it. Plaintiff Bushek entrusted ABC with her PII with the understanding that ABC

[12] *Id.*

[13] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

would keep her information secure and would employ reasonable and adequate data security measures to ensure that her PII would not be compromised.

24. Plaintiff Bushek has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

25. As a direct and traceable result of the Data Breach, Plaintiff Bushek suffered actual injury and damages after her PII was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of her bargain because ABC did not adequately protect her PII; (d) emotional distress because identity thieves now possess her first and last name paired with her Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and published on the dark web; (f) diminution in the value of her PII, a form of intangible property that ABC obtained from Plaintiff Bushek and/or her medical providers; and (g) other economic and non-economic harm.

26. Plaintiff Bushek has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII stolen in the Data Breach.[14]

27. Plaintiff Bushek has a continuing interest in ensuring that her PII, which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches. Absent Court intervention, Plaintiff Bushek's PII will be wholly unprotected and at-risk of future data breaches.

[14] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

C. Cybercriminals Will Use the PII Obtained in the Breach to Defraud Plaintiff and the Class.

28. PII is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

29. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[15] For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[16] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

30. Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[17]
>
> (Emphasis added.)

---

[15] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[16] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[17] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

31. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[18]

32. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running a targeted cyberattack against companies like ABC is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[19] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[20]

33. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, they ***will*** use it.[21]

34. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

---

[18] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[19] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[20] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[21] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[22] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

35. For instance, with a stolen Social Security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[23]

36. The ramifications of Defendant' failure to keep its Class Members' PII secure are long lasting and severe. Once that information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

37. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

38. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened. [24] This gives thieves ample time to, for example, seek multiple medical treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[25]

39. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[26]

---

[23] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[24] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[25] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[26] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

40. As a direct and proximate result of the Data Breach, Plaintiff and the Class have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of further harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, following Federal Trade Commission checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

41. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property including PII;

c. Improper disclosure of their PII;

d. Publication of their PII on the dark web;

e. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and having been already misused;

f. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII and that identity thieves have already used that information to defraud other victims of the Data Breach;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

g. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

i. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class members' personal information for which there is a well-established and quantifiable national and international market;

j. The loss of use of and access to their credit, accounts, and/or funds;

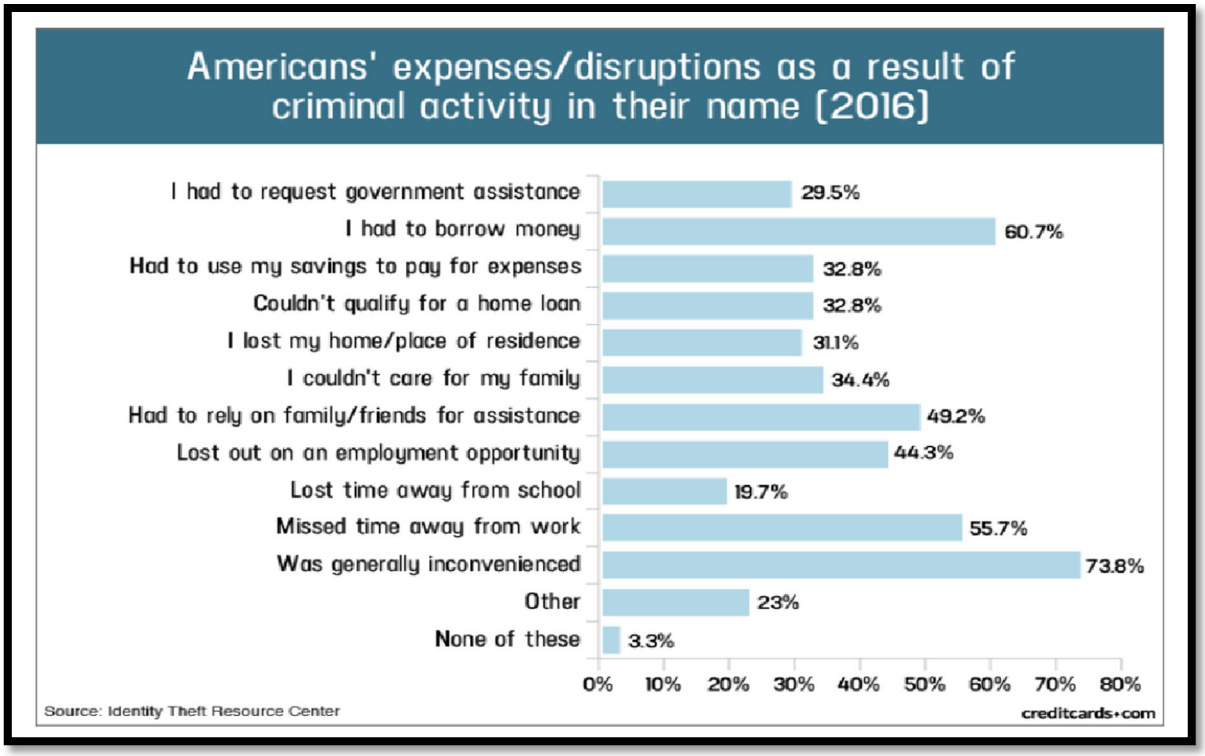
k. Damage to their credit due to fraudulent use of their PII; and

l. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

42. Below is a chart that shows the kinds of expenses and disruptions that victims of identity theft experience[27]:

[27] Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com



43. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiff's PII.

44. Plaintiff and Class Members also have an interest in ensuring that their PII that was provided to ABC is removed from ABC's unencrypted files.

45. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiff and Class Members an inadequate 12 or 24 months of identity theft repair and monitoring services. This limited identity theft monitoring is, however, inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk.[28]

[28] *See* Ex. 1.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

46. The letters acknowledged that the Data Breach would cause inconvenience to affected individuals by providing numerous actions for Class Members to take in an attempt to mitigate the harm caused by the Data Breach and that financial harm would likely occur.

47. At ABC's suggestion, Plaintiff is desperately trying to mitigate the damage that ABC has caused him. Given the kind of PII ABC made accessible to hackers, however, Plaintiff is certain to incur additional damages. Because identity thieves have her PII, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[29]

48. None of this should have happened, the Data Breach was preventable.

D. Defendant were Aware of the Risk of Cyber Attacks

49. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some

[29] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

of the biggest cybersecurity breaches: Target,[30] Yahoo,[31] Marriott International,[32] Chipotle, Chili's, Arby's,[33] and others.[34]

50. ABC should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the PII that it collected and maintained.

E. Defendant Could Have Prevented the Data Breach.

51. Data breaches are preventable.[35] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[36] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[37]

---

[30] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[31] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[32] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[33] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[34] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[35] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[36] *Id.* at 17.

[37] *Id.* at 28.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

52. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[38]

53. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[39] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

54. Upon information and belief, ABC failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, ABC also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

---

[38] *Id.*

[39] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

55. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[40]

56. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

[40] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[41]

57. Further, to prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

[41] *Id.* at 3-4.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[42]

58. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**

  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials

- **Thoroughly investigate and remediate alerts**

  - Prioritize and treat commodity malware infections as potential full compromise;

[42] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

- **Include IT Pros in security discussions**
    - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
    - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
    - Monitor for adversarial activities
    - Hunt for brute force attempts
    - Monitor for cleanup of Event Logs
    - Analyze logon events
- **Harden infrastructure**
    - Use Windows Defender Firewall
    - Enable tamper protection
    - Enable cloud-delivered protection
    - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[43]

59. Given that Defendant was storing the PII of many individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

60. Specifically, among other failures, ABC had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.[44]

61. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all confidential information. Further,

[43] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[44] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

the Data Breach could have likely been prevented had Defendant utilized appropriate malware prevention and detection technologies.

62. ABC was negligent in its failure to ensure it had proper security measures in place to store Plaintiff's and Class Members' confidential PII.

F. Defendant's Response to the Data Breach is Inadequate.

63. Defendant failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

64. Defendant stated that the Data Breach was discovered in or around August 2024—months after Defendant notified Plaintiffs and the Class of the Data Breach. Even then, Defendant failed to inform Plaintiff and Class Members exactly what information was exposed in the Data Breach, leaving Plaintiff and Class Members unsure as to the scope of information that was compromised.

65. During these intervals, the cybercriminals were exploiting the information while ABC was secretly still investigating the Data Breach.

66. If ABC had investigated the Data Breach more diligently and reported it sooner, Plaintiff and the Class could have taken steps to protect themselves sooner and to mitigate the damages caused by the Breach.

IV. CLASS ACTION ALLEGATIONS

67. Plaintiff incorporates by reference all preceding paragraphs as if fully restated herein.

68. Plaintiff brings this action against ABC and ABC on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class and the state subclass (collectively, the "Class") defined as follows:

Nationwide Class
All persons whose PII was compromised as a result of the Data Breach.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

69. Excluded from the Class is Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

70. Plaintiff reserves the right to amend the above definitions or to propose additional subclasses in subsequent pleadings and motions for class certification.

71. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

72. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. The class is comprised of over 39,000 people.

73. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through ABC's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of ABC.

74. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

75. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress ABC's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

76. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's PII;

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PII, and whether it breached this duty;

d. Whether Defendant breached their duties to Plaintiff and the Class as a result of the Data Breach;

e. Whether Defendant failed to provide adequate cyber security;

f. Whether Defendant knew or should have known that its computer and network security systems were vulnerable to cyber attacks;

g. Whether Defendant conduct, including their failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether ABC was negligent in permitting unencrypted PII of vast numbers of individuals to be stored within its network;

i. Whether ABC was negligent in permitting unencrypted PII of vast numbers of individuals to be stored within ABC's network;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

j. Whether Defendant were negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees, applicants, and business associates;

k. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

l. Whether ABC continues to breach duties to Plaintiff and the Class;

m. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant' negligent actions or failures to act;

n. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

o. Whether Defendant' actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

V. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of all Plaintiff and the Class)

77. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

78. Defendant ABC solicited, gathered, and stored the PII of Plaintiff and the Class.

79. Defendant had full knowledge of the sensitivity of the PII it maintained and of the types of harm that Plaintiff and Class Members could and would suffer if their PII were wrongfully disclosed. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Members had no ability to protect their PII that was in ABC's possession. As such, a special relationship existed between ABC and the Plaintiff and the Class.

80. Defendant was well aware of the fact that cybercriminals routinely target organizations through cyberattacks in an attempt to steal the collected PII.

81. Defendant owed Plaintiff and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing PII, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

82. Defendant's duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

83. Defendant had duties to protect and safeguard the PII of Plaintiff and the Class from being vulnerable to cyberattacks, including, by encrypting documents containing PII, by not permitting documents containing unencrypted PII to be maintained on its systems, and other similarly common-sense precautions when dealing with sensitive PII. Additional duties that ABC owed Plaintiff and the Class include:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

b. To protect the PII in its possession using reasonable and adequate security procedures and systems;

c. To adequately and properly audit and test its systems;

d. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

e. To adequately and properly audit, test, and train its employees regarding how to avoid phishing attempts and scams;

f. To train its employees not to store PII for longer than absolutely necessary;

g. To implement processes to quickly detect a data breach, security incident, or intrusion; and

h. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

84. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating special relationships between them and ABC. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiff and the Class had entrusted to it.

85. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit and test its computer systems to avoid cyberattacks;

d. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII, including maintaining it in an encrypted format;

e. Failing to adequately and properly audit, test, and train its employees regarding how to avoid phishing attempts and scams

f. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's PII;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

h. Failing to abide by reasonable retention and destruction policies for PII it collects and stores; and

i. Failing to promptly and accurately notify Plaintiff and Class Members of the Data Breach that affected their PII.

86. Defendants' willful failures to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

87. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

88. The damages Plaintiff and the Class have suffered (as alleged above) were and are reasonably foreseeable.

89. The damages Plaintiff and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

90. Plaintiff and the Class have suffered injury, including as described above, and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

91. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

92. Through the use of Plaintiff's and Class Members' PII, Defendant received monetary benefits.

93. Defendant collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff and Class Members.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

94. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

95. However, acceptance of the benefit under the facts and circumstances described herein, make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, ABC instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

96. Under the principle of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members because ABC failed to implement the appropriate data management and security measures, and ABC failed to ensure the appropriate data management and security measures were in place.

97. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

98. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to allow Defendant to have or maintain their PII.

99. As a direct and proximate result of ABC's decision to profit rather than provide adequate data security, and as a direct and proximate cause of ABC's failure to ensure it provided adequate data security, Plaintiff and Class members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs ABC reasonably should have expended on data security measures to secure Plaintiff's PII, (ii) time and expenses mitigating harms, (iii) diminished value of the PII, (iv) harms as a result of identity theft; and (v) an increased risk of future identity theft.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

100. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

101. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

102. Plaintiff incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

103. Defendant required Plaintiff and Class Members to provide services and/or employment. In exchange, Defendant entered into implied contracts with Plaintiff and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class members' PII and to timely notify them in the event of a data breach.

104. Plaintiff and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

105. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

106. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

107. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class members.

FOURTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of Plaintiff and the Class)

108. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

109. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

110. As previously alleged and pleaded, Defendant owed duties of care to Plaintiff and Class Members that required it to adequately secure their PII.

111. Defendant still possesses the PII of Plaintiff and the Class Members.

112. Defendant has not satisfied its obligations and legal duties to Plaintiff and the Class Members.

113. ABC has claimed that it is taking some steps to increase its data security, but there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Breach, and to once again place profits above protection.

114. Plaintiff, therefore, seeks a declaration (1) that ABC's existing security measures do not comply with its obligations and duties of care to provide adequate security, and (2) that to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant' systems on a periodic basis,

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering Defendant to significantly increase its spending on cybersecurity including systems and personnel;

c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;

d. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

e. Ordering that Defendant segment Plaintiff's and the Class's PII by, among other things, creating firewalls and access controls so that if one area of Defendant' systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

f. Ordering that Defendant cease storing unencrypted PII on its systems;

g. Ordering that Defendant conduct regular database scanning and securing checks;

h. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

i. Ordering Defendant to implement and enforce adequate retention policies for PII, including destroying, in a reasonably secure manner, PII once it is no longer necessary for it to be retained; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Complaint.

Dated: December 20, 2024

Respectfully Submitted,

By: /s/ *Samuel J. Strauss*

Samuel J. Strauss, WSBA #46971
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109

sam@straussborrelli.com

William B. Federman*
Kennedy M. Brian*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
kpb@federmanlaw.com

**pro hac vice request* forthcoming

Counsel for Plaintiff and the Putative Class

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com